Anneaux

1) On munit l'ensemble $A = \mathbb{Z} \times \mathbb{Z}$ des deux lois internes

$$(a,b) + (a',b') = (a+a', b+b') \quad \text{et} \quad (a,b) \,.\, (a',b') = (aa', 0)$$

Montrer que $(A,+,.)$ est un anneau commutatif non unitaire. Quels sont les diviseurs de 0 dans A ?.

2) On note cette fois-ci $E = \mathbb{Z} \times \mathbb{Z}$ et l'on définit les opérations internes

$$(a,b) + (a',b') = (a+a', b+b') \quad \text{et} \quad (a,b) \,.\, (a',b') = (aa' - bb', ab' + ba')$$

Montrer que $(E,+,.)$ est un anneau commutatif unitaire. Est-il intègre ? Déterminer les diviseurs de l'unité dans E.

3) L'anneau des entiers de Gauss est $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \,/\, a, b \in \mathbb{Z}\}$. Vérifier que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ et qu'il est isomorphe à B.

Solution :

[0] [uann0008] Dany-Jack Mercier

Exercice : a) On note $A = \mathbb{Z}\times\mathbb{Z}$. On munit A des 2 lois

$$(a,b)+(a',b') = (a+a', b+b') \quad \text{et} \quad (a,b).(a',b') = (aa', 0)$$

Montrer que A est un anneau commutatif et trouver tous les diviseurs de 0.

b) On pose cette fois-ci :

$$(a,b)+(a',b') = (a+a', b+b') \quad \text{et} \quad (a,b).(a',b') = (aa'-bb', ab'+ba')$$

Montrer que A est un anneau commutatif unitaire. Est-il intègre ?
Déterminer les diviseurs de l'unité.

Sol. : a) $aa'=0$ donc ~~les diviseurs de 0 de A sont ...~~ tous les él. de A ~~diviseurs~~ sont des div. de 0. En effet : $\forall (a,b)\in A$ tq $(a,b)(0,1)=(0,0)$

b) Notons $\mathbb{1} = (a',b')$ l'unité de A. On aura :

$$\begin{cases} aa'-bb'=a \\ ab'+ba'=b \end{cases} \forall a,b \Rightarrow \begin{cases} a'=1 \\ b'=0 \end{cases} \qquad \text{Donc } \boxed{\mathbb{1}=(1,0)}$$

* A intègre ?

$$(1)\ \begin{cases} aa'-bb'=0 \\ ab'+ba'=0 \end{cases} \Rightarrow abb'+b^2a'=0 \qquad \text{donc } a^2a'+b^2a'=0$$

$$a'(a^2+b^2)=0$$

d'où $a'=0$ si $(a,b)\neq(0,0)$.

Mais alors, (1) donne : $\begin{cases} bb'=0 \\ ab'=0 \end{cases} \Rightarrow b'=0.$

Ainsi, si $(a,b).(a',b')=0$ et $(a,b)\neq(0,0)$ on a : $(a',b')=(0,0)$ ie A intègre.

* Diviseurs de $\mathbb{1}$?

$$\begin{cases} aa'-bb'=1 & (2) \\ ab'+ba'=0 & (3) \end{cases}$$

- Si $a\neq 0$, $b'=-\dfrac{a'}{a}b$ donc $aa'+b\dfrac{a'}{a}b=1 \Rightarrow \begin{cases} a'=\dfrac{a}{a^2+b^2} \\ b'=-\dfrac{b}{a^2+b^2} \end{cases}$

Comme $a'\in\mathbb{Z}$, cela entraine $\begin{cases} a=\pm1 \\ b=0 \end{cases}$, mais alors (3) donne $\begin{cases} a'=\pm1 \\ b'=0 \end{cases}$ ← ordre à respecter

Ainsi $\boxed{(\pm1,0).(\pm1,0)=\mathbb{1}}$

- Si $a=0$ et $a'=0$, (2) et (3) s'écrivent : $bb'=-1$ ie $\begin{cases} (0,1)(0,-1)=\mathbb{1} \\ \text{ou} \\ (0,-1)(0,1)=\mathbb{1} \end{cases}$

Conclusion : Les diviseurs de $\mathbb{1}$ sont de la forme $(0,\pm1)$ ou $(\pm1,0)$.

Soit a un élément d'un anneau principal A. Montrer que :

1) a est irréductible si, et seulement si, a est premier avec tout nombre qu'il ne divise pas.

2) a est irréductible si, et seulement si, il vérifie l'assertion suivante :

$$a|bc \Rightarrow a|b \text{ ou } a|c$$

Solution :

[0] [uann0012] Dany-Jack Mercier

Soit A un anneau principal.
Mq :

a) a irréductible $\Leftrightarrow$ a est premier avec tout nbre qu'il ne divise pas

b) a irréductible $\Leftrightarrow$ $\{ a | pq \Rightarrow a|p$ ou $a|q \}$

---

a) ($\Rightarrow$) Si $a \nmid b$ et si d est un diviseur commun à a et b, $d|a$ donc $d = au$ ou u (avec $u \in A^*$).

$d = au$ est impossible (sinon $a|d|b$) donc $d = u \in A^*$

On a montré : $d|a$ et $d|b \Leftrightarrow d \in A^*$

ie $a \wedge b = 1$

($\Leftarrow$) Soit $a = pq$.

Si $a|p$, $p = aa'$ et $a = aa'q \Rightarrow 1 = a'q \Rightarrow q \in A^*$

Si $a \nmid p$, $a \wedge p = 1$ et le Th. de Gauss entraîne $a|q$. On montre alors que $p \in A^*$ comme ci-dessus.

b) ($\Rightarrow$) Si a irréductible, soit $a|pq$. a est premier avec tout él. qu'il ne divise pas, donc :

si $a \nmid p$ alors $a \wedge p = 1$ et le Th. de Gauss entraîne $a|q$

($\Leftarrow$) Si $a = pq$, alors $a|pq$ donc $a|p$ ou $a|q$

Supposons $a|p$. On aura $p = au$ et $a = auq \Rightarrow 1 = uq \Rightarrow \begin{cases} u \in A^* \\ q \in A^* \end{cases}$

donc p est irréductible.

Anneaux de fractions $S^{-1}A$.
Soit A un anneau commutatif et unitaire, mais non nécessairement intègre. Une partie S de A est dite multiplicative si elle vérifie

$$1 \in S,\ 0 \notin S \text{ et } \forall x \in S \quad \forall y \in S \quad xy \in S.$$

1) Soit $\mathcal{R}$ la relation dans l'ensemble $A \times S$ définie par

$$\forall (a,s), (a',s') \in A \times S \quad (a,s)\,\mathcal{R}\,(a',s') \Leftrightarrow \exists t \in S \quad (as' - sa')\,t = 0.$$

Montrer que $\mathcal{R}$ est une relation d'équivalence. On notera $\frac{a}{s}$ la classe d'équivalence du couple (a,s), et $S^{-1}A$ l'ensemble quotient $A \times S/\mathcal{R}$. Vérifier que les lois

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + sa'}{ss'} \text{ et } \frac{a}{s} \times \frac{a'}{s'} = \frac{aa'}{ss'}$$

définissent sur une structure d'anneau. Vérifier que l'application $i : A \to S^{-1}A$ définie par $i(a) = \frac{a}{1}$ est un morphisme d'anneaux. Est-il injectif ?
2) A partir de cette question et jusqu'à la fin du problème, on suppose que l'anneau A est intègre. Quelle simplification cela entraine-t'il dans la définition de $\mathcal{R}$? Que devient l'application i ? Peut-on considérer A comme un sous-anneau de $S^{-1}A$?
3) Si R est un anneau, on note $\mathcal{P}'_A$ l'ensemble des idéaux premiers de A n'interceptant pas S, et $\mathcal{P}_{S^{-1}A}$ l'ensemble des idéaux premiers de $S^{-1}A$. Montrer que l'application

$$\begin{array}{rccc} \Phi : & \mathcal{P}'_A & \to & \mathcal{P}_{S^{-1}A} \\ & I & \mapsto & S^{-1}I = \left\{ \frac{i}{s} \,/\, i \in I \text{ et } s \in S \right\} \end{array}$$

est bijective croissante d'inverse $J \mapsto J \cap A$.
4) **Anneau local.** De façon générale et si A est un anneau intègre, montrer l'équivalence entre les propriétés :
  i) A ne possède qu'un seul idéal maximal,
  ii) l'ensemble $A \backslash A^*$ des éléments non inversibles de A forme un idéal.
Lorsque l'une des propriétés ci-dessus est vérifiée, on dit que A est un anneau local, et l'on remarque qu'alors l'unique idéal maximal $\mathcal{M}$ de A est $\mathcal{M} = A \backslash A^*$.
5) Soit t un élément non nul d'un anneau intègre A et $S_t = \{1, t, t^2, ...\}$.
  a) Montrer que S_t est une partie multiplicative de A. On pose

$$A_t = S_t^{-1}A = \left\{ \frac{a}{t^n} \in \text{Frac}(A) \,/\, a \in A \text{ et } n \in \mathbb{N} \right\}$$

où Frac(A) désigne le corps des fractions de A.
  b) Supposons maintenant que $A = \mathbb{Z}$ et que t soit un nombre entier premier. Expliciter le groupe multiplicatif $\mathbb{Z}_t^*$ et montrer que l'anneau $\mathbb{Z}_t$ est local. Quels sont les idéaux premiers de $\mathbb{Z}_5$?
  c) Décrire les idéaux premiers de $\mathbb{Z}_{42}$.
6) Soit t un élément non nul de l'anneau intègre A.
  a) Montrer qu'il y a correspondance bijective entre les idéaux premiers de A_t et les idéaux premiers de A ne contenant pas t.
  b) Montrer qu'il y a correspondance bijective entre les idéaux premiers de $A/(t)$ et les idéaux premiers de A contenant t.
  c) Quels sont les idéaux premiers de $\mathbb{Z}/42\mathbb{Z}$?
7) Soit I un idéal premier d'un anneau intègre A.
  a) Montrer que la partie $S_I = A \backslash I$ est multiplicative. On pose $A_I = S_I^{-1}A$.
  b) Montrer que l'anneau A_I est local.
  c) Quels sont les idéaux premiers de $\mathbb{Z}_{(5)}$? de $\mathbb{Z}/5\mathbb{Z}$?

[0][uann0019] Dany-Jack Mercier (réf. Milne p12 par exemple)

1) Il est facile de voir que $\mathcal{R}$ est Réflexive et Symétrique. Montrons la transitivité. Il faut prouver que

$$\left.\begin{array}{l}(a,s)\,\mathcal{R}\,(a',s')\\(a',s')\,\mathcal{R}\,(a'',s'')\end{array}\right\} \Longrightarrow (a,s)\,\mathcal{R}\,(a'',s'')$$

Supposons donc qu'il existe $t, u \in S$ tq

$$\begin{cases}(as'-sa')t=0\\(a's''-s'a'')u=0\end{cases}$$

Cela entraîne

$$\begin{cases}(as''s'-ss''a')tu=0\\(a'ss''-s'sa'')ut=0\end{cases}$$

$$\overline{\quad(as''-sa'')s'ut=0\quad}$$

et prouve bien que $(a,s)\,\mathcal{R}\,(a'',s'')$.

(---)

> $\frac{a}{s}\cdot\frac{b}{s'} \in S^{-1}I \Leftrightarrow \frac{ab}{ss'}=\frac{i}{s''}$ $i \in I$
>
> $\Rightarrow abs''=ss'i \in I \Rightarrow a \in I$ ou $b \in I$ (puisque hyp $\Rightarrow s'' \notin I$)

2) (...)

3) Φ est bien définie car $S^{-1}I$ est un idéal premier de $S^{-1}A$ dès que I est un idéal premier de A.

On suppose ici que $A \subset S^{-1}A$ via le monomorphisme $i : A \to S^{-1}A$.

Si J est un idéal de $S^{-1}A$, alors $J \cap A$ sera un idéal de A.

Il reste à montrer que :

$$\begin{cases}(1) \quad S^{-1}I \cap A = I \quad \forall I \in \mathcal{P}'_A\\(2) \quad S^{-1}(J\cap A) = J \quad \forall J \in \mathcal{P}_{S^{-1}A}\end{cases}$$

<u>Preuve de (1)</u> : $S^{-1}I \cap A \supset I$ est trivial. Réc., si $x \in S^{-1}I \cap A$, alors $x = \frac{i}{s} = a \in A$ où $i \in I$ et $s \in S$. Donc $i = as \in I \Longrightarrow a \in I$ ou $s \in I$ (puisque I est premier). Comme par hypothèse $s \notin I$, on déduit $a \in I$.

<u>Preuve de (2)</u> : Si $J \in \mathcal{P}_{S^{-1}A}$, et si $x \in J$, alors $x = \frac{a}{s}$ avec $a = xs \in J \cap A$. L'inclusion $J \subset S^{-1}(J\cap A)$ est donc vraie. Réc., si $x \in S^{-1}(J \cap A)$, alors $x = \frac{a}{s}$ avec $a \in J\cap A$ et $s \in S$. Donc $a = xs \in J \cap A$, et cela entraîne $x \in J$ ou $s \in J$ (puisque J est premier). Comme $s \notin J$ (car [illegible]) on déduit $x \in J$. □

4.a)

4) Si A ne possède qu'un seul idéal maximal $\mathfrak{M}$, alors bien sûr $\mathfrak{M} \subset A \setminus A^*$. Mais tout élément x de $A \setminus A^*$ est inclus dans un idéal maximal, donc ici $x \in \mathfrak{M}$. On a montré que $\mathfrak{M} = A \setminus A^*$ et que $A \setminus A^*$ était un idéal.

Réc. si $A \setminus A^*$ est un idéal et si $\mathfrak{M}$ est un idéal maximal, $\mathfrak{M}$ est inclus dans $A \setminus A^*$ (sinon $\mathfrak{M} \cap A^* \neq \emptyset \Rightarrow \mathfrak{M} = A$ absurde). La maximalité de $\mathfrak{M}$ entraîne alors $\mathfrak{M} = A \setminus A^*$.

5.a)

5.b) • $\mathbb{Z}_t = \left\{ \frac{a}{t^n} \in \mathbb{Q} \ / \ a \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$

• $\frac{a}{t^n} \in \mathbb{Z}_t^* \iff \exists b \in \mathbb{Z} \ \exists m \in \mathbb{N} \quad \left(\frac{a}{t^n}\right)\left(\frac{b}{t^m}\right) = 1$

$\iff \exists b \in \mathbb{Z} \ \exists m \in \mathbb{N} \quad ab = t^{n+m}$

$\iff \exists s \in \mathbb{N} \quad a = \pm t^s$

mq $\boxed{\mathbb{Z}_t^* = \{ \pm t^k \ / \ k \in \mathbb{Z} \}}$

• $\underline{\mathbb{Z}_t \text{ est local}}$: en effet $\mathbb{Z}_t \setminus \mathbb{Z}_t^*$ est un idéal. Pour le voir, il faut prouver l'implication

(*) $\quad \forall x = \frac{a}{t^n} \in \mathbb{Z}_t \setminus \mathbb{Z}_t^* \text{ et } \forall y = \frac{b}{t^m} \in \mathbb{Z}_t \Rightarrow xy \in \mathbb{Z}_t \setminus \mathbb{Z}_t^*$

Par l'absurde : si l'on suppose $xy = \frac{ab}{t^{n+m}} \in \mathbb{Z}_t^*$, alors $ab = \pm t^s$ $(s \in \mathbb{N})$ donc, puisque t est premier, $b = \pm t^{s'}$ $(s' \in \mathbb{N})$. Cela entraîne $b \in \mathbb{Z}_t^*$ et c'est contraire à l'hypothèse. □

• $\mathbb{Z}_5 = \left\{ \frac{a}{5^n} \in \mathbb{Q} \ / \ a \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$ et les idéaux premiers de $\mathbb{Z}_5$ s'écrivent $S_5^{-1} I$ où I est un idéal premier de $\mathbb{Z}$ ne coupant pas S_5 (cf 2). Donc $I = 0$ ou $I = (p)$ avec p premier et $p \neq 5$. Les idéaux premiers de $\mathbb{Z}_5$ seront :

(0), (2), (3), (7), (11), ...,

5.c) Les idéaux premiers de $\mathbb{Z}_{42}$ seront : $(0), (5), (11), (13), \ldots$ d'après la question 2).

6.a) La bijection est $I \longmapsto S_t^{-1} I$ (donnée en 2))

et dire que $I \cap S_t = \emptyset$ équivaut à dire que $t \notin I$ (car I premier !)

6.b) On utilise un résultat connu : il y a bijection entre les idéaux premiers de $A/_{(t)}$ et les idéaux premiers de A contenant (t), et cette bijection est donnée par :

$$I \longmapsto \pi(I)$$

où $\pi : A \longrightarrow A/_{(t)}$ est la projection canonique. La bijection réciproque est $J \longmapsto \pi^{-1}(J)$.

6.c) Les idéaux premiers de $\mathbb{Z}/_{42\mathbb{Z}} = \mathbb{Z}/_{(42)}$ sont :

$$(0), (2), (3), (7)$$

7.a) (...)

7.b) <u>A_I est local ?</u>

- $A_I = \left\{ \frac{a}{s} \ / \ a \in A \text{ et } s \notin I \right\}$
- $A_I^* = \left\{ \frac{a}{s} \ / \ a \notin I \text{ et } s \notin I \right\}$. En effet :

$\frac{a}{s} \in A_I^* \iff \exists b \in A \ \exists s' \notin I \quad \frac{ab}{ss'} = 1$

$\iff \exists b \in A \quad \exists s' \notin I \quad ab = ss' \notin I$ (cf I premier)

$\implies a \notin I$.

Réc., si $a \notin I$ et $s \notin I$, alors $\frac{a}{s} \times \frac{s}{a} = 1$ donc $\frac{a}{s} \in A_I^*$.

• $A_I \setminus A_I^* = \{ \frac{a}{s} \,/\, a \in I \text{ et } s \notin I \}$ sera un idéal puisque :

$\forall a \in I \; \forall b \in A \quad \forall s, s' \notin I \qquad \frac{a}{s} \cdot \frac{b}{s'} = \frac{ab}{ss'} \in A_I \setminus A_I^*$ (car $ab \in I$).

Cela prouve que A_I est un <u>anneau local</u>..

7.c)

$$\mathbb{Z}_{(5)} = \left\{ \frac{a}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}} \in \mathbb{Q} \;/\; a \in \mathbb{Z} \text{ et } p_1, \ldots, p_k \text{ premiers différents de } 5,\ \alpha_1, \ldots, \alpha_k \in \mathbb{N},\ k \in \mathbb{N}^* \right\}$$

Les idéaux premiers de $\mathbb{Z}_{(5)}$ seront des $S_{(5)}^{-1} I$ où I est un idéal premier de $\mathbb{Z}$ ne coupant pas $S_{(5)} = A \setminus (5)$, ie inclus dans (5) (d'après 2)). Ce sera donc les idéaux :

$$\boxed{(0)\,,\,(5)}.$$

Les idéaux premiers de $\mathbb{Z}/5\mathbb{Z}$ seront : $\boxed{(0) \text{ et } (5)}$ (cf 5.c)).

FIN

Soit A un anneau non réduit à $\{0\}$, dont A et $\{0\}$ sont les seuls idéaux à gauche.

a) Mq pour tout $a \in A$, la translation à dte $\delta_a : x \mapsto xa$ est soit nulle, soit bijective.

b) Supposons qu'il existe $a_0 \in A$ tq δ_{a_0} soit non nulle. Montrer l'existence d'un unique élément e de A tel que $ea_0 = a_0$. Prouver que $\forall x \in A \quad xe = x$ puis que $ex = x$ (on pourra considérer l'ensemble des éléments de la forme $x - ex$ pour démontrer ce dernier point)

c) En déduire que A est soit un anneau de carré nul (ie $\forall x, y \in A \quad xy = 0$) soit un corps.

---

a) * $\mathrm{Im}\,\delta_a = \{xa \,/\, x \in A\}$ est un idéal à gauche de A puisque $0 = 0a \Rightarrow 0 \in \mathrm{Im}\,\delta_a$, et :

* $\forall xa, ya \in \mathrm{Im}\,\delta_a \quad xa - ya = (x-y)a \in \mathrm{Im}\,\delta_a$
* $\forall y \in A \quad \forall xa \in \mathrm{Im}\,\delta_a \quad y.xa = (yx)a \in \mathrm{Im}\,\delta_a$

Donc $\mathrm{Im}\,\delta_a = \{0\}$ ou $\mathrm{Im}\,\delta_a = A$, ie $\delta_a = 0$ ou δ_a surjective.

* Si $\delta_a \neq 0$, δ_a sera donc surjective. δ_a est un endomorphisme du groupe additif $(A, +)$, donc $\mathrm{Ker}\,\delta_a$ est un sous-groupe de $(A,+)$. En fait, $\mathrm{Ker}\,\delta_a = \{x \,/\, xa = 0\}$ est un idéal à gauche de A, donc $\mathrm{Ker}\,\delta_a = \{0\}$ ou A. Comme $\delta_a \neq 0$, $\mathrm{Ker}\,\delta_a \neq A$, donc $\mathrm{Ker}\,\delta_a = \{0\}$ et δ_a sera injectif.

* Conclusion : $\delta_a = 0$ ou δ_a bijectif.

b) D'après le a), δ_{a_0} étant bijectif, il existera un et un seul élément e tel que $ea_0 = a_0$.

Par suite : $\forall x \in A \quad xea_0 = xa_0$ ce qui entraîne $\boxed{xe = x}$ (puisque δ_{a_0} injectif).

* $J = \{x - ex \,/\, x \in A\}$ est un idéal à gauche car :

1) $0 - e0 = 0 \in J$
2) $(x-y) - e(x-y) = x - ex - (y - ey) \in J$ dès que $x - ex$ et $y - ey \in J$
3) $\forall y \in A \quad \forall x - ex \in J \quad y(x - ex) = yx - \underset{y}{\underline{ye}}x = yx - yx = 0 \in J$

donc $J = \{0\}$ ou A.

Si $J = A$, il existerait $x_0 \in A$ tel que $x_0 - ex_0 = a_0 \Rightarrow e(x_0 - ex_0) = ea_0$
$\Rightarrow 0 = a_0$ absurde.

Donc $J = \{0\}$ ie $\forall x \in A \quad x - ex = 0$

Ccl : Si $\delta_{a_0} \neq 0$, A est un anneau unitaire, d'unité e.

c) Si $\exists x, y \in A \quad xy \neq 0$ alors $\exists a_0 \in A \quad \delta_{a_0}$ non nulle

On peut appliquer le b) : A sera un anneau unitaire, d'élément unité e.
$A \neq \{0\}$ entraîne $e \neq 0$.

$\forall x \in A \setminus \{0\} \quad ex = x \neq 0$ donc δ_x n'est pas nulle, donc δ_x sera bijective (cf a)) et l'équation en y : $yx = e$ admettra une unique solution x'.

<u>x' sera l'inverse à gauche de x ie $x'x = e$</u>.

Montrons que x' sera aussi inverse à dte de x : pour cela, notons x'' l'inverse à gauche de x'. On a :

$$x''x' = e \quad \text{et} \quad x''x'x = x''e \Rightarrow ex = x'' \Leftrightarrow x = x''$$

donc bien $xx' = e$.

<u>Ccl</u> : <u>A sera un anneau unitaire dont tout élément non nul possède un inverse</u>. Ce sera <u>un corps</u>.